UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/919,248	07/31/2001	John Holden Bickford	RSW920010143US1	2799

30449 7590 10/07/2008

SCHMEISER, OLSEN & WATTS
22 CENTURY HILL DRIVE
SUITE 302
LATHAM, NY 12110

EXAMINER	
PYZOCHA, MICHAEL J	
ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
10/07/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte JOHN HOLDEN BICKFORD,
CHARLES STEVEN LONGAFELT, and ROBERT B. SISK

Appeal 2007-1336
Application 09/919,248
Technology Center 2100

Decided: October 7, 2008

Before RICHARD TORCZON, SALLY C. MEDLEY, and JAMES MOORE, *Administrative Patent Judges*.

MEDLEY, *Administrative Patent Judge*.

DECISION ON APPEAL

A. Statement of the Case

International Business Machines Inc. ("IBM"), the real party in interest, seeks review under 35 U.S.C. § 134(a) of a Final Rejection of claims 3-11 and 13-20, the only claims remaining in the application on appeal. We have jurisdiction under 35 U.S.C. § 6(b). We affirm-in-part.

The application on appeal was filed 31 July 2001.

The Examiner relies on the following prior art in rejecting the claims on appeal:

Liu et al. ("Liu")	6,760,752 B1	July 6, 2004
Lindeman et al. ("Lindeman")	2003/0009698 A1	Jan. 9, 2003
Leeds	2002/0016824 A1	Feb. 7, 2002

The Examiner rejected claims 8, 9, 13, and 14 under 35 U.S.C. § 102(e) as anticipated by Lindeman.

The Examiner rejected claims 3-5, 15, 17, 18, and 20 under 35 U.S.C. § 103(a) as unpatentable over Lindeman and Leeds.

The Examiner rejected claims 6, 7, 10, 11, 16, and 19 under 35 U.S.C. § 103(a) as unpatentable over Lindeman, Leeds, and Liu.

B. Findings of Fact ("FF")

Lindeman

1. Lindeman describes a process for spam filtering e-mail messages.
2. The process includes receiving a new e-mail message (fig. 7, step 702) and determining whether there is a tunnel password in the message (fig. 7, step 704). ¶¶ 95-99, fig. 7.
3. If a tunnel password is present in the message (yes branch of step 704), the message is left in the user's inbox (step 706). ¶ 99, fig. 7.

4. If the tunnel password is not present (no branch of step 704), a determination is made if a CZID[1] is in the message (step 708). ¶ 101, fig. 7.
5. The CZID is an MD5 (Message Digest 5) hash of the original sender address, original destination address and secret string. ¶¶ 0031-0032.
6. The CZID is included in the message and used to authenticate the message, source e-mail address and destination e-mail address. ¶¶ 0031-0032.
7. If the CZID is present (yes branch of step 708), the process proceeds to steps 710 and 712 for further authentication. ¶ 101, fig. 7.
8. If the CZID is not present (no branch of step 708), a determination is made whether the sender is trusted (step 716). ¶ 104, fig. 7.

Leeds

9. Leeds describes a junk e-mail filtering system. ¶ 36.
10. Users are provided with an authentication code certifying that they are not known spammers. ¶ 36.
11. E-mail users register and are assigned a unique identification code. ¶ 37.
12. The user's e-mail program maintains the unique code in secret so that users and others will not see the message (including the code). ¶ 37.
13. When a message is received, the mail program or mail handling system at the ISP (Internet Service Provider) or corporate level sends the unique code and the "From:" identifier to the authenticator for authentication. ¶ 37.

---

[1] A CZID is defined as a unique ID for an email message ¶ 0111. The meaning of CZ is unclear. Our best guess is that CZ stands for CascadeZone Inc. which is listed as Lindeman's assignee.

14. The code and "From:" identifier are checked against the database of known junk e-mailers and checked for consistency between the two parts. ¶ 37.
15. Following authentication, the e-mail program or e-mail handling system at the ISP or corporate level strips the unique code before delivering the message to the recipient. ¶ 37.
16. Stripping the unique code prior to delivering the message to the recipient prevents the recipient from stealing a unique code of the message sender. ¶ 37.

C. Principles of Law

"Anticipation under 35 U.S.C. § 102(e) requires that 'each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.'" *In re Robertson*, 169 F.3d. 743, 745 (Fed. Cir. 1999) (citation omitted).

> If the prior art reference does not expressly set forth a particular element of the claim, that reference still may anticipate if that element is 'inherent' in its disclosure. To establish inherency, the extrinsic evidence 'must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill.' 'Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient.'

Id. (citations omitted).

Argument of counsel cannot take the place of evidence lacking in the record. *Meitzner v. Mindick,* 549 F.2d 775, 782 (CCPA 1977); *In re Pearson*, 494 F.2d 1399, 1405 (CCPA 1974).

In *KSR International Co. v. Teleflex Inc*, the Supreme Court explained that despite the enactment of Section 103 and the *Graham*[2] analysis there still remains "the need for caution in granting a patent based on the combination of elements found in the prior art." 127 S.Ct. 1727, 1739 (2007). Based on its precedent, the Court reaffirmed the principle that "[t]he combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." *Id.*

> When a work is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or a different one. If a person of ordinary skill can implement a predictable variation, § 103 likely bars its patentability. For the same reason, if a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill. [A] court must ask whether the improvement is more than the predictable use of prior art elements according to their established functions.
>
> *Id.* at 1740.

---

[2] *Graham v. John Deere Co*, 383 U.S. 1 (1966). Under the *Graham* analysis, "[t]he scope and content of the prior art are ... determined; differences between the prior art and the claims at issue are ... ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background the obviousness or nonobviousness of the subject matter is determined. Such secondary considerations as commercial success, long felt but unsolved needs, failure of others, etc., might be utilized to give light to the circumstances surrounding the origin of the subject matter sought to be patented." *KSR*, 127 S.Ct. at 1730 (ellipses in original).

D. Analysis

Rejection of claims 8, 9, 13, and 14 as anticipated by Lindeman

Claims 8, 9, 13, and 14 are independent. App. Br. 36-41. Claim 8 is representative and recites "determining whether an authentication key is expected to be present in an open field of the electronic mail". App. Br. 38.

The Examiner finds that Lindeman inherently determines whether an authentication key (e.g., CZID) is expected to be present through the step of determining whether a tunnel password is present (step 704). Ans. 11, 13, 16-17, 19-20; citing Lindeman fig. 7. According to the Examiner, if the tunnel password is present, no CZID is expected to be present, but if the tunnel password is not present, the CZID is expected to be present. Ans. 11, 13, 16-17, 19-20; citing Lindeman ¶¶ 98-100.

IBM argues that it does not necessarily and inevitably follow that if a tunnel password is not present, the CZID is expected to be present and if the tunnel password is present, the CZID is not expected to be present. Reply Br. 4-5, citing Lindeman ¶¶ 98-100, fig. 7. We agree.

Lindeman does not explicitly or inherently describe determining whether a CZID is expected to be present. If a tunnel password is present (fig. 7, step 704) then the presence or absence of the CZID is irrelevant. The message is left in the user's inbox whether a CZID is present or not (step 706). FF[3] 3. Thus, no determination of whether the CZID is expected is made. Conversely, if a tunnel password is not present, then it does not necessarily follow that a CZID is expected. Again, no such determination of whether the CZID is expected is made. The system has no such expectation as exemplified by checking if a CZID is present or not (yes branch of 708 and

[3] FF denotes Finding of Fact.

no branch of 708). FFs 3-4. The Examiner has not shown that the Lindeman system, either explicitly or inherently, determines whether a CZID is expected to be present.

For these reasons, the Examiner erred in finding claims 8, 9, 13, and 14 anticipated by Lindeman.

Rejection of claims 17, 18, and 20 as obvious over Lindeman and Leeds

Claims 17, 18, and 20 are dependent on, and include all the limitations of, claims 8, 9, and 13 respectively. App. Br. 41. As applied by the Examiner, Leeds does not make up for the deficiencies of Lindeman. We find that the Examiner erred in determining that claims 17, 18, and 20 are obvious over Lindeman and Leeds.

Rejection of claims 10, 11, and 19 as obvious over Lindeman, Leeds and Liu

Claims 10, 11, and 19 are dependent on, and include all the limitations of, claim 9. App. Br. 39, 41. As applied by the Examiner, neither Leeds nor Liu make up for the deficiencies of Lindeman. We find that the Examiner erred in determining that claims 10, 11, and 19 are obvious over Lindeman, Leeds, and Liu.

Rejection of claims 3-5 as obvious over Lindeman and Leeds

IBM argues claims 3-5 together as a group. App. Br. 22-24 and Reply Br. 10-12. Independent claim 3 is representative and recites "storing an authentication key associated with an originator in a memory of the originator . . . ". App. Br. 36.

The Examiner finds that the user of the e-mail program is the "originator." The Examiner further finds that each user and each e-mail program has a unique authentication code that is stored in the memory of the

originator and that the unique code is read from memory and included in a message. Ans. 23, citing Leeds ¶¶ 36-37.

IBM agrees that Leeds describes an authentication key associated with the originator, but disagrees that the key is "stored in a memory of the originator". Reply Br. 10-12. IBM argues that Leeds' e-mail handling system and authenticator need to store the secret unique identifier (i.e., authentication key) in their respective memories, but the originator has no need to store the secret unique identifier in the originator memory. Reply Br. 11.

Leeds describes both an e-mail program that belongs to a user (i.e., sender, originator) and an e-mail program or e-mail handling system at the ISP or corporate level. FFs 10-13, 15. The Examiner focuses on Leeds' description of the e-mail program at the user's level (i.e. the sender or originator). IBM focuses on Leeds' description of an e-mail handler or program at an ISP or corporate level. For the reasons that follow, IBM has failed to show error in the Examiner's finding that the authentication key associated with the originator is stored in a memory of the originator.

Leeds describes that e-mail users register and are assigned a unique identification code. FF 11. Importantly, Leeds describes that the e-mail program *maintains the unique code in secret by the mail program* so that users and others will not see the message (which includes the unique identification code). FF 12. To "maintain" the code means to keep it or store it.

We find that in order for the sender's (i.e., originator's) e-mail program to maintain the unique code in secret by the mail program, the unique code must be stored by the sender's (i.e., originator's) e-mail program. This is

further bolstered by the fact that the mail handler at the ISP level receives the code. FF 13. If users (e.g., originators) and others do not see the message with the unique code, but yet the ISP mail handler receives the unique code, it necessarily follows that the user's e-mail program stores the unique code and sends the message including the code to the ISP mail handler.

IBM's argument that it is obvious not to store Leeds' secret unique identifier in the memory of the originator for security reasons (Reply Br. 11) is misplaced. As explained above, Leeds does describe the disputed limitation. Similarly, IBM argues that it would not have been obvious to modify Lindeman to store the CZID (i.e., authentication key) in the memory of the originator for security reasons. Reply Br. 11-12. However, IBM has not directed us to evidence in support of its arguments. We do not know, since IBM has failed to explain, with supporting evidence, why storing the CZID in the memory of the originator would raise any security concerns. Argument of counsel cannot take the place of evidence lacking in the record. In any event, any security concerns would be addressed by Leeds description that the unique identifier is stored *in secret* by the user's e-mail program. FF 12.

IBM further argues that the Examiner's combination of Lindeman and Leeds is improper since Leeds does not teach that storing and reading an authentication key in the originator's memory facilitates determining when e-mail is junk e-mail. App. Br. 24. IBM argues that instead Leeds describes that the authenticator would receive information about whether a message is junk e-mail while the message is in the inbox, similar to Lindeman's determination of when e-mail is junk. App. Br. 24. IBM misapprehends the

Leeds reference. Leeds describes that the determination of junk e-mail is necessarily performed by reading the unique code stored in the sender's e-mail program and ultimately sending a message with the code to an authenticator where it is checked against a database of known junk e-mailers. FFs 10-14. Leeds' description about receiving additional information while the message is in the inbox is merely an additional detection means. That detection means enables a junk e-mail message to be called back from the recipient's inbox if it is later discovered to be junk e-mail following an initial check. ¶ 36.

IBM also argues that Leeds teaches away from storing and reading the authentication key in a memory of the originator because Leeds describes that the database of junk e-mailers is stored in a memory of the authenticator. App. Br. 24. The argument is not persuasive. As explained before, Leeds describes that the originator's e-mail program must store the unique code in the memory of the originator's e-mail program in order to maintain the unique code in secret.

For all these reasons, we find that IBM has not sustained its burden of establishing that the Examiner erred in determining that claims 3-5 are obvious over Lindeman and Leeds.

Rejection of claim 15 as obvious over Lindeman and Leeds

Claim 15 is dependent on claim 3, and further recites "the authentication key is dependent only upon an identity of the originator." App. Br. 41. The Examiner finds that the combination of Lindeman and Leeds describes the disputed limitations. Final Rejection 7, Ans. 7, citing Leeds ¶¶ 36-37. The Examiner further finds that creating a CZID dependent upon only the identity of the originator would not destroy the Lindeman reference because

authentication of the message and the recipient can be performed by other well-known cryptographic methods, such as digital signatures. Ans. 24.

IBM argues that modifying Lindeman with the teaching of Leeds would destroy Lindeman's CZID. IBM argues that the CZID is essential to Lindeman's invention because the CZID is necessary to authenticate the confirmation message. Reply Br. 12. IBM further argues that decapitating the original destination address and secret string from the CZID would change the CZID so drastically that the resulting CZID would no longer relate to Lindeman's invention. Reply Br. 13.

We are unpersuaded by IBM's arguments. IBM has not explained, with supporting evidence, why one of ordinary skill in the art would consider the Lindeman and Leeds combination to be unsuitable. We will simply not take counsel's word that the combination would change the CZID drastically or destroy the CZID as asserted. Moreover, IBM has not shown error with the Examiner's finding that authentication of the message and the recipient can be performed by other well-known cryptographic methods. Modifying the Lindeman's CZID with Leeds' authentication code that is dependent only upon the identity of the originator is no more than a predictable use of prior art elements according to their established functions. In such a case, when a person of ordinary skill in the art can implement a predictable variation, section 103 likely bars patentability. IBM has not directed us to any evidence to the contrary.

For all these reasons, we find that IBM has not sustained its burden of establishing that the Examiner erred in determining that claim 15 is obvious over Lindeman and Leeds.

Rejection of claims 6-7 and 16 as obvious over Lindeman, Leeds, and Liu

Representative claim 6 is independent and recites "storing an authentication key in a memory of a recipient of the electronic mail . . . " and "reading the stored authentication key from the address at the memory of the recipient, and comparing the authentication key with the stored authentication key . . . " . App. Br. 37. The Examiner relies on Leeds for the disputed limitations. Ans. 27, citing Leeds ¶¶ 36-37. IBM disagrees that Leeds describes the disputed claim limitations. App. Br. 27-29 and Reply Br. 15, 19.

Although Leeds describes that the users and their e-mail program are provided with a unique identification code maintained (i.e. stored) by the e-mail program (FFs 10-12), the Examiner has not directed us to, and we can not find, where Leeds describes that the code is also stored in or read from a recipient's memory. In fact, Leeds describes that the authentication or unique identification code does not even reach the recipient. Specifically, Leeds describes that before passing an e-mail message to a recipient, the unique code in the e-mail message can be stripped from the message to prevent the recipient from stealing the unique code of the sender. FFs 15-16.

For all these reasons, we find that the Examiner erred in determining that claims 6-7 and 16 are obvious over Lindeman, Leeds, and Liu.

E. Decision

Upon consideration of the appeal, and for the reasons given herein, it is

ORDERED that the decision of the Examiner rejecting claims 8, 9, 13, and 14 under 35 U.S.C. § 102(e) as anticipated by Lindeman is reversed.

ORDERED that the decision of the Examiner rejecting claims 3-5 and 15 as unpatentable under 35 U.S.C. § 103(a) over Lindeman and Leeds is affirmed.

ORDERED that the decision of the Examiner rejecting claims 17, 18, and 20 as unpatentable under 35 U.S.C. § 103(a) over Lindeman and Leeds is reversed.

ORDERED that the decision of the Examiner rejecting claims 6, 7, 10, 11, 16, and 19 as unpatentable under 35 U.S.C. § 103(a) over Lindeman, Leeds, and Liu is reversed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a).

AFFIRMED IN-PART

ack

cc:

SCHMEISER, OLSEN & WATTS
22 CENTURY HILL DRIVE
SUITE 302
LATHAM NY 12110